CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

ETHI • NUMÉRO 112 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 7 juin 2018

Président

M. Bob Zimmer

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le jeudi 7 juin 2018

● (0850)

[*Traduction*]

Le président (M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC)): Je déclare ouverte la 112e séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, conformément au sous-alinéa 108(3)h)(vii), étude de l'atteinte à la sécurité des renseignements personnels associée à Cambridge Analytica et Facebook.

Monsieur Vickery, heureux de vous revoir. Je vous remercie de comparaître encore une fois aujourd'hui devant notre comité.

M. Chris Vickery (directeur de la recherche sur les risques cybernétiques, UpGuard, à titre personnel): Je me réjouis de participer.

Le président: Nous allons commencer notre premier tour avec M. Erskine-Smith, pour sept minutes.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Merci, monsieur Vickery.

J'ai vraiment une question fondamentale. Avez-vous examiné le disque dur dont vous nous avez parlé lors de votre dernière comparution?

M. Chris Vickery: Il y a tant de choses là-dessus que je suis sûr que je n'en ai pas encore observé tous les recoins, mais oui, j'en ai examiné une très grande partie.

M. Nathaniel Erskine-Smith: Vous avez assurément une expertise que le Comité n'a pas en ce qui concerne l'examen de ce matériel. Dans la mesure où vous n'avez pas tout regardé — vous en avez examiné une grande partie — à la lumière de cet examen, pouvez-vous nous fournir les faits saillants de ce que vous avez découvert qui serait à votre avis pertinent pour le Comité, particulièrement compte tenu du fait qu'AIQ comparaîtra devant nous la semaine prochaine?

M. Chris Vickery: Oui. Quand je réfléchis à la vue d'ensemble globale, le thème prépondérant fondamental qui me vient à l'esprit, c'est qu'on semble déployer des efforts considérables pour faire en sorte que les choses ne soient pas facilement examinables en ce qui concerne l'historique des recherches sur Internet, l'historique des transactions et les données: où cela s'en va, où c'est compilé et agrégé, et au moment d'attribuer des sources à chaque chose. Il semble se dégager un thème courant: on rassemble beaucoup de choses, puis on les laisse se désagréger d'une façon qui n'est pas facilement vérifiable. On pourrait le faire à des fins de sécurité. On pourrait le faire à des fins de dissimulation. Cela me rend toutefois très méfiant.

Par exemple, il y a dans le projet éphémère — le nom « éphémère » vous donne en quelque sorte une idée — un thème sous-jacent: on utilise des canaux et le WebSocket de manière à communiquer dans le plus grand secret. Cela ne veut pas dire, à première vue, que c'est nécessairement quelque chose de malveillant, mais c'est fait de telle façon qu'il devient très difficile de prouver au-delà de tout doute qu'une certaine transaction a été réalisée par des moyens convenables réguliers.

M. Nathaniel Erskine-Smith: Je vois quelques-uns de vos gazouillis qui disent qu'AIQ a une application Facebook, que l'entreprise usurpait des numéros de téléphone américains et qu'elle communiquait avec des électeurs américains. Ce sont deux exemples que j'ai vus dans certains de vos commentaires publics. Y a-t-il d'autres exemples que vous avez tirés du matériel que nous devrions connaître?

M. Chris Vickery: Oui. Je lui demanderais très précisément pourquoi un développeur a dit qu'elle devait supprimer des données qui auraient été recueillies en contravention des lois sur la protection des renseignements personnels du Royaume-Uni. De toute évidence, c'est presque un aveu de culpabilité. Si vous avez recueilli quelque chose en contravention des lois sur la protection des renseignements personnels du Royaume-Uni et que vous vous en débarrassez, pourquoi l'avez-vous fait en premier lieu?

M. Nathaniel Erskine-Smith: Qui était l'auteur de la déclaration?

M. Chris Vickery: Je crois que c'était un commentaire anonyme, pour autant que je sache. Je pourrais peut-être retourner voir qui travaillait sur ce projet, qui aurait probablement formulé le commentaire, mais il me faudrait faire quelques recherches.

M. Nathaniel Erskine-Smith: Lors de votre première comparution, vous aviez d'abord réagi en disant que des renseignements avaient été compilés à partir d'un certain nombre de sources différentes et vous aviez fait allusion à l'entrepôt de données du RNC. Je pense que vous aviez même mentionné les frères Koch. Après un examen plus approfondi, avez-vous une idée globale de l'endroit d'où provient toute l'information?

M. Chris Vickery: Je connais beaucoup de sources. Je ne peux pas dire en toute certitude que c'est exhaustif, parce que, bien sûr, les sources ont elles-mêmes des sources. Par exemple, i360 est le nom de l'entreprise financée ou dirigée par les frères Koch qui fournit des tonnes de données. Manifestement, l'entrepôt de données du RNC est une grande fondation d'où on obtient de l'information ou des données. En ce qui concerne les noms de champ, il y a des indices selon lesquels L2 Political a fourni des renseignements, et je crois que, sur le blogue du site Web de Cambridge Analytica — pas le site Web d'AIQ — on admet que la source était L2.

Axiom était une source, je crois, qui a été mentionnée hier dans le témoignage d'Alexander Nix. Lorsque je regroupe les données d'AIQ et de Cambridge Analytica, je vois tellement d'interactions entre les deux qu'il est simplement inévitable que les ensembles de données soient interreliés, sans mentionner que clairement, les identificateurs de SCL figurent dans les noms de champ de bon nombre des importations.

M. Nathaniel Erskine-Smith: C'est là où je veux en venir avec ma question. Ce qui a déclenché l'enquête, ici et dans le monde, c'est la collecte et la communication inappropriées d'information entre Facebook, Kogan et SCL. Nous parlons maintenant d'au moins 87 millions d'utilisateurs de partout dans le monde et de plus de 600 000 au Canada. Selon vous, à la lumière de votre examen de la base de données, il ne fait aucun doute qu'AIQ a accédé à cette information et qu'elle faisait partie de cet ensemble de données principal.

M. Chris Vickery: C'est possible, et permettez-moi de vous expliquer pourquoi. Dans le projet Ripon, on tient un certain type de journal des erreurs résiduelles lorsque quelque chose a mal tourné durant une importation, et le journal a consigné ce qui s'est produit. Ce journal des erreurs d'importation, pour autant que je sache, contient quelques exemples de ce que le système importait de serveurs appelés SCLCruiseRipon.com, je crois.

On y trouve des notes psychographiques OCEAN, et celles-ci provenaient d'un domaine qui est enregistré sous le nom d'Alexander Nix. Je ne sais pas d'où ils obtenaient ces notes psychographiques. Ce n'est pas chaque entrée unique qui en avait, mais c'était le cas d'un bon nombre d'entre elles. Dans les scripts qui les extraient, il y a un petit champ « si disponible » à côté de la note psychographique. S'il y en a un bon nombre qui s'assortissent de notes psychographiques et un bon nombre dont ce n'est pas le cas, cela soulève la question de savoir s'ils avaient extrait les données de ces 87 millions d'utilisateurs et s'il s'agissait de celles qui comportaient les notes psychographiques.

● (0855)

M. Nathaniel Erskine-Smith: Si SCL et Nix sont mêlés à cela, c'est loin d'être une simple possibilité: il serait même probable que cette base de données découle de cette information.

M. Chris Vickery: Je suis d'accord. C'est probable. Je n'ai pas de communications spéciales de leur part qui le confirment, mais je suis très méfiant.

M. Nathaniel Erskine-Smith: C'est tout pour moi.

Le président: Passons maintenant à M. Gourde pour sept minutes.

[*Français*]

M. Jacques Gourde (Lévis—Lotbinière, PCC): Merci, monsieur le président.

Monsieur Vickery, vous avez parlé de rassemblement de données. Quel genre de données sur la vie privée des gens retrouve-t-on dans ce logiciel?

[*Traduction*]

M. Chris Vickery: Quels types de champs? Est-ce la question?

[*Français*]

M. Jacques Gourde: Tout à l'heure, vous avez dit qu'on avait supprimé des données sur la vie privée. En quoi consistaient ces données? Était-ce des numéros de téléphone, des dates de naissance, des numéros de comptes bancaires?

[*Traduction*]

M. Chris Vickery: Il me faudrait retourner examiner ce script. Il s'intitulait « *salt the earth* », et je me rappelle le commentaire qu'on avait formulé, parce qu'il me trotte dans la tête: une personne a dit que cela aurait pu contrevenir aux lois sur la protection des renseignements personnels du Royaume-Uni, mais je n'ai pas en tête les champs exacts qui étaient alors éliminés.

[*Français*]

M. Jacques Gourde: Ce que vous nous avez fourni semble assez compliqué à comprendre. Est-ce le codage ou la façon dont c'est organisé qui fait que c'est plus difficile à comprendre?

[*Traduction*]

M. Chris Vickery: C'est peut-être en partie difficile à comprendre parce que c'est le disque dur exact, ou une copie de celui-ci, que j'ai fourni au comité du Royaume-Uni. Dans la séance privée du comité du Royaume-Uni, j'ai pu expliquer un peu les choses et fournir un certain contexte. C'est peut-être ce qui explique une partie de la confusion, puisque je ne me suis pas assis avec vous pour vous donner un peu de contexte. Cela prête peut-être un peu aussi à confusion, parce que ce n'est pas un logiciel inutilement intuitif de type « clic, clic, clic » ou « fenêtre, fenêtre, fenêtre ». Vous devez connaître un peu Git, les logiciels de décompression et le développement Web pour vous faire une idée de l'interaction entre un bon nombre de ces fichiers et la façon dont le logiciel enregistre et structure le travail.

[*Français*]

M. Jacques Gourde: Ce logiciel pourrait-il être fourni au Comité pour que nous puissions comprendre ce qu'il y avait dans le disque dur?

[*Traduction*]

M. Chris Vickery: Oui, ce sont des logiciels libres et ouverts. Je peux vous en fournir la liste. Si vous avez une équipe de techniciens déjà en place, je suis sûr qu'ils seront en mesure de s'y mettre directement.

[*Français*]

M. Jacques Gourde: Ce logiciel s'est-il retrouvé entre les mains de plusieurs compagnies ou seulement de quelques-unes d'entre elles, de façon restrictive?

[*Traduction*]

M. Chris Vickery: Je pense la réponse ici est double. Certains logiciels sont des cadres qui sont ouverts et accessibles à quiconque dans le monde, puis il y a des projets qui sont créés à partir de ce logiciel ouvert qu'AIQ a conçu.

Parlez-vous de ceux conçus par AIQ, créés à partir des cadres, ou de ceux qui sont ouverts et accessibles à tout le monde?

[*Français*]

M. Jacques Gourde: En fait, je ne parlais pas du logiciel, mais plutôt de l'information qui se trouvait dans ce disque dur et que vous nous avez fournie. Cette information s'est-elle retrouvée entre les mains de plusieurs entreprises ou bien d'une seule compagnie en particulier qui a au moins tenté de préserver la confidentialité de l'information?

● (0900)

[*Traduction*]

M. Chris Vickery: Le disque dur que vous avez est extrait directement de GitLab, à l'adresse gitlab.aggregateiq.com. Il s'agit des données détenues par AggregateIQ. Toutefois, l'entreprise a incorporé beaucoup de scripts et de logiciels qui sont accessibles sur l'Internet ouvert.

Je pense que la réponse à votre question, c'est qu'il s'agit de données internes d'AggregateIQ. La réponse philosophique globale, c'est que n'importe qui dans le monde aurait pu y avoir accès, parce que c'était ouvert et exposé du côté d'AIQ et parce que l'entreprise l'a conçu en utilisant un logiciel, principalement des cadres, qui sont accessibles au public. C'est une réponse double.

[*Français*]

M. Jacques Gourde: Le niveau de sécurité que cette compagnie a accordé aux données personnelles sur ce disque dur était-il élevé, moyen ou médiocre?

[*Traduction*]

M. Chris Vickery: En ce qui concerne ce que je vous ai remis, le degré de sécurité était nul. Il n'y avait aucune mesure de sécurité que ce soit qui le protégeait. Je n'y attribuerais aucun niveau de sécurité. Il y a des noms d'utilisateur, des mots de passe et des emplacements réseau qui auraient pu être vus par n'importe qui dans le monde entier.

[*Français*]

M. Jacques Gourde: C'est incroyable. Donc, tous les renseignements contenus dans ces disques durs auraient pu se retrouver entre les mains de n'importe qui ayant eu un intérêt à les utiliser à d'autres fins, tout simplement.

[*Traduction*]

M. Chris Vickery: Exactement. Oui, c'est ce qui est très dérangeant.

[*Français*]

M. Jacques Gourde: Merci. J'ai terminé.

[*Traduction*]

Le président: Merci, monsieur Gourde.

Passons maintenant à M. Boulerice. Vous avez sept minutes.

[*Français*]

M. Alexandre Boulerice (Rosemont—La Petite-Patrie, NPD): Merci beaucoup, monsieur le président.

Monsieur Vickery, merci beaucoup de comparaître encore une fois devant notre comité, seulement quelques mois après votre dernière comparution.

On a beaucoup parlé de Cambridge Analytica, d'AIQ et de SCL. Selon vous, quelle est l'ampleur de ce monde souterrain d'échange de données qui peuvent être utilisées à des fins politiques? Parle-t-on de ces entités simplement parce qu'on est tombé dessus par hasard ou parce qu'il y a eu quelques lanceurs d'alerte? Y a-t-il seulement ces entités ou est-ce la pointe de l'iceberg d'un phénomène beaucoup plus vaste et plus large que ce que l'on pourrait l'imaginer?

[*Traduction*]

M. Chris Vickery: Je crois que ce que vous venez de dire est probablement la vérité, que c'est le début de quelque chose de beaucoup plus vaste. Même si ce n'est que le tout début, je crois qu'il y a une assez bonne chance que nous découvrions, avant que ce soit terminé, des liens avec d'autres pays qui n'ont pas vraiment été reconnus dans les médias, ainsi que divers groupes d'intérêts spéciaux aux États-Unis — peut-être au Canada, mais assurément au sein des États-Unis — qui ont tiré profit de cet ensemble de données, peut-être en ne sachant pas exactement d'où il provenait. Je crois qu'il y a ici une très grande machine au travail, et nous n'en avons pas vu tous les aspects.

[*Français*]

M. Alexandre Boulerice: Selon vous, comment pourrait-on, à titre d'État et de gouvernement, chercher et trouver les autres organismes ou entreprises qui échangent ou utilisent des données de cette façon, à des fins politiques, pour s'ingérer dans des campagnes électorales? Doit-on enclencher une grande chasse à l'homme?

[*Traduction*]

M. Chris Vickery: Je crois que la meilleure façon de voir les choses, ce serait peut-être essentiellement la même que celle utilisée par le passé par les États-Unis pour débusquer des familles de la mafia. Vous exercez des pressions sur des gens contre qui vous avez de fortes preuves, vous les amenez à se retourner contre leurs complices et à obtenir de l'information privilégiée, et continuez de faire tomber les dominos jusqu'au bout de la chaîne, jusqu'à ce que toute la vérité sorte. C'est fait d'une telle façon que c'est difficile, à moins de disposer d'information confidentielle ou de découvrir une erreur énorme comme celle que j'ai découverte. C'est difficile d'amener l'information confidentielle dans les mains des enquêteurs.

● (0905)

[*Français*]

M. Alexandre Boulerice: Cependant, selon ce que vous dites, une fois qu'une brèche a été faite, on peut s'en servir pour creuser et trouver toutes les ramifications.

[*Traduction*]

M. Chris Vickery: Je crois que nous avons une tête de pont, si c'est ce dont vous parlez, afin de créer une brèche, autrement dit, pour vraiment commencer à creuser davantage. Oui, je crois que nous avons pratiqué une brèche.

[*Français*]

M. Alexandre Boulerice: Merci.

Ma question suivante, je la pose plutôt du point de vue du Parlement canadien, ou peut-être d'Élections Canada. Nous tenons à l'intégrité de notre système électoral. Nous ne voudrions pas voir des puissances étrangères s'ingérer dans nos campagnes électorales et utiliser les données personnelles de nos citoyens pour influencer le comportement électoral, la perception des gens, voire le résultat des élections.

Toutefois, j'ai l'impression que les États sont des institutions très lourdes et très lentes. Ici, par exemple, les députés devaient, jusqu'à tout récemment, envoyer des autorisations au moyen de télécopies. C'est un peu comme si nous courrions en patins à roulettes derrière une Ferrari et que nous étions constamment en retard.

Quel conseil nous donneriez-vous pour que nos lois visant à protéger nos citoyens soient à jour et adaptées?

Ici, tout le processus est un peu archaïque. Il n'est pas très moderne et il est assez lent, en général.

[*Traduction*]

M. Chris Vickery: Je crois qu'un aspect, propre au côté canadien des choses, vous procure vraiment un avantage: AggregateIQ relève de la compétence canadienne. Si vous pouvez faire toute la lumière sur la participation d'AggregateIQ à toute cette situation, vous pourrez vraiment aller au fond de l'affaire et vous dire: « D'accord, ils ont fait ça. Comment aurions-nous pu prévoir cela? Comment aurions-nous pu voir quelques signaux d'alarme? Qu'ont-ils fait et comment sont-ils arrivés à ce niveau de participation sans qu'on le sache? » Ensuite, vous pourrez colmater les brèches afin d'empêcher que ce genre de choses se produisent dans l'avenir.

Je crois que, à cet égard, vous vous trouvez en réalité dans une position de pouvoir.

[*Français*]

M. Alexandre Boulerice: C'est bon à savoir. Merci.

Pensez-vous que les solutions se trouvent davantage du côté des enquêtes ou plutôt du côté des protections légales ou législatives?

[*Traduction*]

M. Chris Vickery: Je crois que la réglementation, comme [*Difficultés techniques*] sera très utile pour protéger le public contre les abus. Si le Canada souhaite vraiment examiner le modèle du RGPD, y adhérer et faire adopter quelque chose de son cru, je suis très en faveur d'une réglementation qui a du mordant, pour que cela soit appliqué. Lorsqu'il y a une violation flagrante d'une loi qui est mise en place, faites des entreprises qui sont les violatrices flagrantes un exemple et faites craindre aux autres de faire la même chose.

[*Français*]

M. Alexandre Boulerice: C'est un peu comme ce que vous disiez tout à l'heure sur la façon de s'attaquer aux familles de la mafia.

Monsieur le président, combien de temps de parole me reste-t-il?

[*Traduction*]

Le président: Vous avez environ 30 secondes.

[*Français*]

M. Alexandre Boulerice: Vous êtes aux États-Unis et nous sommes au Canada. Comment qualifieriez-vous notre niveau de sécurité pour ce qui est de l'intégrité de notre système électoral? Est-ce que les choses vont bien ou est-ce que nous sommes de toute évidence menacés?

[*Traduction*]

M. Chris Vickery: J'ai une question rapide. Le Canada envisage-t-il d'instaurer des votes par téléphone ou Internet?

[*Français*]

M. Alexandre Boulerice: Non, pas encore.

[*Traduction*]

M. Chris Vickery: D'accord. Tenez-vous-en loin. Utilisez des bulletins de vote avec des pistes de vérification. Tant et aussi longtemps que vous utiliserez des bulletins de vote avec des pistes de vérification, vous serez relativement sur la bonne voie.

[*Français*]

M. Alexandre Boulerice: Merci beaucoup, monsieur Vickery.

[*Traduction*]

Le président: C'est maintenant au tour de M. Saini, pour sept minutes.

M. Raj Saini (Kitchener-Centre, Lib.): Bonjour monsieur Vickery. J'aimerais donner suite à certaines questions posées par mon collègue, M. Erskine-Smith, juste à des fins de précision.

Vous avez découvert des preuves qu'AIQ a usurpé des numéros de téléphone avec identification de l'appelant dans des appels faits à des électeurs américains. Pouvez-vous nous expliquer les preuves et dire pourquoi c'est un problème pour eux?

● (0910)

M. Chris Vickery: Dans le commentaire sur les développeurs qui s'écrivent, on dit qu'ils établissent l'identité de l'appelant différemment de ce qui se fait en vérité, parce que s'ils appellent quelqu'un, cela leur permet d'acheminer vers une ligne différente la personne qui rappelle à ce numéro. Cela pourrait être un message sur une boîte vocale ou autre chose — l'appel n'est simplement pas acheminé vers le même numéro que celui d'où émane l'appel en réalité.

C'est un problème en ce qui concerne les Américains, parce que je crois comprendre que cette capacité est essentiellement réservée aux situations d'application de la loi, du moins ici, aux États-Unis. Ici, quiconque usurpe l'information d'identification de l'appelant pourrait s'exposer à beaucoup de sanctions, du moins si c'est dirigé vers des Américains. Je ne suis ni avocat ni procureur, mais c'est ma compréhension des choses.

M. Raj Saini: Je vais citer votre gazouillis récent selon lequel Chris Wilson, qui est, je crois, bénévole au Leadership Institute, « a une énorme participation dans AggregateIQ ». Pouvez-vous m'expliquer ce que vous entendez par-là?

M. Chris Vickery: Chris Wilson est à la tête de WPA Intelligence, connue anciennement sous le nom de WPA Opinion Research. Les lettres « WP » sont pour Wilson Perkins, je crois, et il est le « W » dans WPA. Ils ont travaillé en étroite collaboration avec AggregateIQ, selon ce que je puis deviner des fichiers de GitLab.

Je crois que si vous parliez avec WPA, on vous dirait plutôt que c'est elle qui a embauché AggregateIQ comme développeur. Ils ont travaillé en étroite collaboration sur des applications pour téléphone. Le projet éphémère est fortement lié à WPA: certains des fichiers Web qui auraient pu servir aux gens qui appelaient faisaient état du fait qu'ils figuraient dans la base de données des électeurs de WPA. De toute évidence, WPA est fortement lié à AIQ, et cette dernière est une sorte de partenaire ou de développeur dont on retient les services, mais il y a là une relation qui devrait, à mon avis, être examinée.

M. Raj Saini: Dans sa biographie, M. Wilson a souligné qu'il possède une certaine expérience en tant que conseiller de campagne en Russie, en Ukraine et en Turquie. Avez-vous des renseignements au sujet de la participation d'AIQ dans l'un de ces pays et des rôles que l'entreprise pourrait avoir joués?

M. Chris Vickery: En fait, M. Wilson a répliqué dans ce fil de gazouillis en affirmant que les activités en Russie et en Turquie dataient d'il y a 20 ans. Personnellement, je viens tout juste de découvrir les activités en Russie et en Turquie dans son passé, donc je ne peux ni confirmer ni nier son affirmation selon lesquelles elles remontent à 20 ans. Je sais qu'il travaille actuellement avec un parti ukrainien, le parti Osnova, et qu'AIQ a en réalité conçu l'application pour téléphone qu'Osnova utilise en ce moment. Je ne suis au courant d'aucun lien direct de la Russie avec AIQ, mais je sais qu'il existe des liens directs avec l'Ukraine.

M. Raj Saini: Une des choses que nous avons entendu dire dans les témoignages, c'est qu'AIQ, SCL et Cambridge Analytica ont participé à de très nombreuses élections partout dans le monde. Ma question est la suivante, et corrigez-moi si j'ai tort: le logiciel qui a été conçu était Ripon. S'agit-il du même logiciel que celui qui a été utilisé partout dans le monde, ou a-t-on conçu différentes itérations ou différents logiciels pour des pays ou des lieux différents où ces entreprises voulaient travailler?

M. Chris Vickery: Pour être clair, Ripon est seulement un des projets. Toutefois, c'était un projet préliminaire, et je crois que bon nombre des projets qui sont présents sur le disque dur que je vous ai remis, par exemple, sont issus de Ripon et ont en quelque sorte évolué pour devenir des petits écosystèmes en soi. Un des thèmes...

M. Raj Saini: On a peut-être fait des versions différentes de ce logiciel et apporté quelques modifications selon l'endroit de travail et les renseignements qu'on devait recueillir, mais ce logiciel est le principal logiciel qu'AIQ a conçu pour Cambridge Analytica, n'est-ce pas?

M. Chris Vickery: Je crois que c'est juste. Je crois qu'un des thèmes récurrents que nous continuons de rencontrer, c'est qu'une bonne partie du logiciel a fait peau neuve, mais le moteur demeure en grande partie le même. C'est quelque chose qu'on a modernisé.

M. Raj Saini: D'accord.

Dans votre analyse du disque dur, avez-vous découvert des preuves ou des indices vous indiquant exactement à quel endroit ou dans quelles administrations ce logiciel ou cette entreprise avait servi?

M. Chris Vickery: Il y a assurément des indices au sujet des États-Unis, du Canada, du Royaume-Uni et de Trinité-et-Tobago. On mentionne l'Australie. Je ne sais pas dans quelle mesure il se passait beaucoup de choses en Australie, le cas échéant, mais on le mentionne assurément.

M. Raj Saini: D'accord.

M. Chris Vickery: À brûle pourpoint, je ne peux pas en trouver d'autres sans faire de recherches plus précises.

Habituellement, lorsque j'examine des atteintes à la protection des données, j'essaie de me concentrer sur des choses qui vont être évocatrices pour des Nord-Américains, parce que c'est difficile de les amener à s'intéresser beaucoup à des lieux très éloignés.

● (0915)

M. Raj Saini: De plus, vous avez récemment découvert un certain nombre d'applications qu'AIQ exécutait sur Facebook, même si elle avait supposément été bannie de la plateforme.

Savez-vous quelles étaient ces applications? Vous a-t-on dit pourquoi Facebook ne les a pas retirées? Croyez-vous qu'il y a toujours des applications d'AIQ qui sont exécutées sur Facebook?

M. Chris Vickery: Je crois qu'il y a probablement toujours des applications influencées par AIQ, voire conçues par l'entreprise, qui sont présentes sur Facebook sous des noms différents. Je crois que c'est probable.

M. Raj Saini: Vous avez également découvert quelques renseignements qui établissent un lien entre AIQ, Alex Jones et *Infowars*. Pouvez-vous nous dire ce que vous avez découvert et ce que ces liens signifient?

M. Chris Vickery: Pour être très clair, le seul lien, c'était vraiment un fichier image qui se trouvait juste à côté d'une autre image pour une organisation qui s'appelle For America. Je sais qu'AIQ a conçu une plateforme pour For America qui permettait de voir diverses choses que disaient les abonnés Facebook et de les recruter. Si AIQ a fait la même chose pour For America que ce qu'elle a fait pour Breitbart, ce qu'elle a bel et bien fait, il est raisonnable de croire qu'elle pourrait avoir fait la même chose pour Infowars, le site Web. Je ne sais pas. Mis à part ce seul fichier image, dont je ne peux expliquer la présence, je ne connais vraiment pas la relation exacte.

M. Raj Saini: Merci beaucoup.

Le président: Nous passons maintenant à M. Aboultaif, pour cinq minutes.

M. Ziad Aboultaif (Edmonton Manning, PCC): Merci.

Je vais poursuivre sur ce sujet un peu, Chris. D'abord, bonjour.

La création de logiciels permet la personnalisation pour une raison précise, dans ces cas précis que nous abordons en ce moment. Si quelqu'un crée un code pour un logiciel particulier afin qu'il soit utilisé comme outil de gestion d'une campagne politique, et pour ce faire, on doit utiliser certaines données fournies au concepteur de logiciel pour lui donner les outils nécessaires au but de ce logiciel, la personne qui conçoit ce logiciel pourra-t-elle le créer sans connaître la provenance des données? Autrement dit, où se trouvent les mesures de sécurité, et ces personnes pourront-elles créer ce logiciel sans connaître la provenance des données?

M. Chris Vickery: De façon théorique, dans le plus fantastique des mondes, vous pourriez créer un logiciel pour gérer un ensemble de données que vous ne possédez pas. Toutefois, c'est juste hypothétique. Ce n'est pas la réalité. Ce n'est pas ce qui se produit dans le développement de logiciels. Si vous voulez développer quelque chose rapidement, de façon rentable et en temps opportun et plaire à vos clients, vous devrez probablement accéder à une grande quantité de données brutes réelles.

Les affirmations selon lesquelles AggregateIQ n'avait pas accès aux ensembles de données brutes, je crois, sont simplement réfutées par ce qui figure dans les fichiers de GitLab, parce qu'il y a des noms d'utilisateur, de mots de passe et des emplacements réseau liés à ce qu'on définit comme des bases de données réelles, pas de fausses bases de données.

Je crois qu'il est très probable qu'AggregateIQ n'avait pas accès à de très vastes ensembles de données brutes.

M. Ziad Aboultaif: Il est donc en réalité très probable que l'accessibilité des données et l'atteinte à la protection des renseignements personnels ne puissent jamais être évitées lorsqu'on se lance dans ce type d'activité.

● (0920)

M. Chris Vickery: Cela peut être évité. Vous devez juste être extrêmement prudent et utiliser quelques mesures de planification préalables afin de concevoir un logiciel avec prudence ou conclure des ententes qui sont strictement respectées et vérifiées après coup pour que vous puissiez vous assurer qu'il n'y a pas eu d'accès non autorisé de la part d'un tiers.

M. Ziad Aboultaif: Merci.

[*Français*]

M. Jacques Gourde: C'est comme le paradoxe de l'oeuf et de la poule. Ces logiciels ont été mis en place parce qu'il y avait un marché potentiel. Il y a sûrement quelqu'un qui a vu un marché potentiel ou alors des commandes ont été données de façon précise pour atteindre un certain but.

Selon vous, est-ce quelqu'un qui a vu un marché potentiel qui a conçu le logiciel en question ou est-ce carrément le contraire, c'est-à-dire que le logiciel a été conçu sur commande?

[*Traduction*]

M. Chris Vickery: Dans cette situation, je crois comprendre qu'il y avait un résultat escompté et que ce logiciel a été conçu pour répondre à ce résultat. Quelques personnes très puissantes voulaient en influencer d'autres, remporter des élections et faire entrer les opinions et les comportements de personnes dans un certain modèle. Des outils étaient nécessaires à cette fin, et ces outils ont donc été créés. C'est ma compréhension des choses, et je crois que c'est le scénario le plus probable.

[*Français*]

M. Jacques Gourde: Selon vous, combien de personnes de plus, en pourcentage, a-t-on réussi à atteindre, à influencer, à faire changer d'avis ou à inciter à aller voter, comparativement à une élection normale?

[*Traduction*]

M. Chris Vickery: Le pourcentage de personnes dans quel pays?

[*Français*]

M. Jacques Gourde: D'autres témoins ont semblé dire que, peu importe le pays, ce système pouvait influencer une masse supplémentaire de personnes et les inciter à voter pour une option différente. En pourcentage, est-ce une augmentation considérable? Cela peut-il jouer entre 2 et 7 %, ou est-ce un peu moins ou un peu plus, selon vous?

[*Traduction*]

M. Chris Vickery: Je suis d'avis que l'opération d'influence ne ciblerait pas nécessairement une population entière, mais un très grand pourcentage de personnes seraient touchées. C'est pourquoi des entreprises comme SCL possèdent des contrats avec des groupes d'opérations psychologiques au Royaume-Uni. Ils influencent un très grand pourcentage de la population et sont en mesure de changer les opinions de, oui assurément, 2 à 7 % des gens. Ils ont assurément tenté de les changer, si ce n'est déjà fait. Il y a un effet sur au moins un petit nombre, oui.

[*Français*]

M. Jacques Gourde: Était-ce un profilage qui ciblait une partie de la population jugée très influençable devant les différentes options, c'est-à-dire tout simplement des gens qui, en temps normal, savent plus ou moins pour qui voter, mais qui vont prendre une décision à la toute fin de la campagne électorale, au point où, si les partis placent de la publicité à répétition au cours des 10 derniers jours d'une campagne, ces gens peuvent vraiment changer la donne?

[*Traduction*]

M. Chris Vickery: Parce que j'ai vu bien plus que cette seule atteinte à la protection des données et que j'en ai vu d'autres liées aux élections, je peux vous dire qu'on choisit les cibles bien avant les 10 jours précédant une élection. Dans les 10 derniers jours, des applications ont été conçues précisément par AIQ pour amener les gens à voter et en faire le suivi le jour du vote.

Je suis désolé; quelle est la question précise?

Le président: Désolé, nous avons dépassé le temps de beaucoup.

Je dois poursuivre.

Le prochain est M. Baylis, pour cinq minutes.

● (0925)

M. Frank Baylis (Pierrefonds—Dollard, Lib.): Merci, monsieur le président.

Monsieur Vickery, d'abord, je tiens à vous remercier d'accomplir ce gros travail et d'être revenu pour nous aider à comprendre tout cela. Nous vous en sommes très reconnaissants.

Vous aviez préparé un ensemble de notes concernant le témoignage d'AIQ, et il était autant mensonger que trompeur. D'abord, je vous demanderais de bien vouloir remettre officiellement ces notes à notre greffier, si vous le pouvez.

M. Chris Vickery: Je peux assurément le faire. Je crois vous les avoir remises à vous précisément, mais oui, je peux les remettre au greffier.

M. Frank Baylis: J'aimerais m'attarder à une partie de ces mensonges et de ces inexactitudes.

Dans un premier temps, M. Massingham a affirmé qu'aucune loi n'avait été violée sur le lieu des activités. C'était une affirmation claire. Vous m'avez fourni des exemples de trois lieux où on a violé des lois. D'abord, on peut parler de la façon dont ils ont composé avec les lois relatives à la collecte de données du Royaume-Uni. Vous avez dit qu'ils avaient en réalité rédigé des notes pour eux-mêmes dans leur code comme quoi cela contrevenait à la loi et qu'ils avaient dû rajuster le tir.

Pourriez-vous préciser vos propos?

M. Chris Vickery: La ligne dans le code dit à quel endroit ils auraient pu contrevenir à la loi sur la protection des renseignements personnels du Royaume-Uni. Elle ne dit pas précisément qu'ils l'ont violée, mais que s'ils l'ont fait, ce code la répare. C'est dans un fichier qui s'appelle « *salt the earth* ».

M. Frank Baylis: Ils savent que s'ils ne contreviennent pas à la loi, ils s'en approchent et ils vont devoir retirer cela. C'est exact.

M. Chris Vickery: C'est ce que je comprends, oui. C'est comme ça que j'interpréterais cette ligne, oui.

M. Frank Baylis: En ce qui concerne l'usurpation de l'identité de l'appelant, ce qu'ils faisaient pour les Américains, cela va à l'encontre de la loi américaine. Je sais que vous n'êtes pas avocat, mais ils étaient au courant et le faisaient. Est-ce exact?

M. Chris Vickery: C'est ce que je comprends, et il y a même un autre commentaire où ils affirment qu'« il n'y a pas de raison » pour laquelle une personne qui se trouve à l'autre bout du monde ne pourrait pas appeler des électeurs et les influencer. En réalité, il y a une raison. C'est illégal qu'un centre d'appels à l'autre bout du monde appelle des électeurs américains pour les influencer.

M. Frank Baylis: Vous avez mentionné un autre aspect qui est une grande préoccupation. Ils ont fait valoir qu'on leur avait seulement donné la base de données des Républicains. Toutefois, lorsque vous examinez cette base de données, elle était bien plus complète et elle renfermait un certain nombre de personnes comme des policiers, des juges et des agents fédéraux — des choses qui ne figurent pas dans l'entrepôt de données des Républicains. Est-ce exact?

M. Chris Vickery: Permettez-moi de clarifier cela. Ces renseignements figurent dans l'entrepôt de données des Républicains. Toutefois, ils dépassent les limites de ce qu'une campagne normale recevrait. Je le sais, parce qu'il y a quelques années, j'ai trouvé une copie de la base de données de l'entrepôt de données des Républicains. J'y ai vu le contenu et vérifié que oui, des juges, des agents fédéraux et des policiers s'y trouvent. Dans la campagne politique régulière qu'on lancerait dans un des États, on n'aurait pas accès à l'information de ces personnes.

M. Frank Baylis: J'ai posé à M. Silvester un certain nombre de questions où il nous a induits en erreur en ce qui concerne l'absence de coordination, ou une coordination, entre ces différents militants de la campagne *Leave* au Royaume-Uni. Lorsque je lui ai demandé comment ils pouvaient tous être au courant de ce groupe, il a répondu qu'il n'y avait pas de collusion, il n'y avait rien. Il a été très clair sur ce point. Cependant, lorsque je lui ai demandé comment ils étaient tous au courant au Royaume-Uni, à l'autre bout du monde, d'une petite opération en Colombie-Britannique, il a parlé du site Web.

Vous avez fait un certain travail durant le vote du Brexit. Vous avez mentionné que le site Web — je veux juste confirmer cela — disait « *AggregateIQ: Changing the way you work with your data* ». Est-ce exact?

M. Chris Vickery: Je crois qu'il y avait neuf mots sur le site Web, et c'étaient ceux-là. Il y avait une phrase de neuf mots et l'adresse courriel d'une personne-ressource. Je pense que c'est très peu probable que les militants de la campagne *Leave* aient découvert l'entreprise et décidé d'utiliser ses services en se fondant sur neuf mots ou sur un site Web vierge.

M. Frank Baylis: C'est ce qu'on veut nous faire croire: qu'ils ont fait une recherche et découvert ce site Web, lu ces neuf mots, communiqué avec l'entreprise par courriel, et que tout cela a été mis en place de façon indépendante.

M. Chris Vickery: Cela me semble peu probable.

M. Frank Baylis: Cela me semble bien plus que peu probable.

J'ai un autre point. M. Silvester a mentionné qu'ils ne recueillent pas de données, mais vous avez étudié un peu le codage. Si je le comprends bien, une partie du codage fait par AIQ vise précisément la collecte de données. Est-ce exact?

M. Chris Vickery: Oui, c'est une pure invention de dire qu'ils ne sont pas des collecteurs de données. Ils en sont vraiment. J'imagine que si vous voulez jouer avec les mots, vous pourriez dire qu'ils ont été embauchés, à certains moments, pour faire de la collecte de données, mais ne se considèrent pas comme des collecteurs de données. Cela ne veut pas dire qu'ils n'en sont pas. Ils ont certainement recueilli des données. C'est un mensonge de dire qu'ils ne l'ont pas fait.

M. Frank Baylis: C'est carrément un mensonge, et ils jouent avec les mots lorsqu'ils disent... Peu importe comment ils veulent y jouer, ils le font. Ils l'ont fait, ils le font. Ils ont clairement dit qu'ils ne le faisaient pas.

● (0930)

M. Chris Vickery: Oui.

M. Frank Baylis: S'ils disent: « Nous ne sommes pas des collecteurs de données, mais quelqu'un nous embauche pour recueillir des données », ils jouent simplement à des jeux. C'est juste ce que nous appelons un mensonge.

M. Chris Vickery: Oui.

Les jeux de mots, des mots ambigus, quoi que ce soit — c'est un mensonge.

M. Frank Baylis: Merci.

Le président: Le prochain est M. Gourde.

[*Français*]

M. Jacques Gourde: Je vais revenir sur la question que M. Boulerice a abordée en parlant de la pointe de l'iceberg.

On sait qu'il y a eu du profilage et que des logiciels sont mis au point pour essayer de catégoriser la population. À votre connaissance, y a-t-il des choses dont le Comité n'a pas parlé, mais qui devraient être portées à son attention? Devrait-il être mis au courant de ce que certaines personnes ont l'intention de faire dans l'avenir? Y a-t-il des logiciels qui sont mis au point dont on ignore la raison d'être actuelle, mais qui pourraient servir lors d'une élection?

[*Traduction*]

M. Chris Vickery: Il y a un logiciel pour les élections. Je ne sais pas s'il a déjà été utilisé quelque part.

Si vous regardez dans le disque dur, il y a une zone qui s'appelle « vb9k » et « vb9k admin », quelque chose du genre. Elle contient le squelette, si ce n'est le prototype de fonctionnement d'un système électoral, à un point tel qu'il y a des scripts pour envoyer à des gens des courriels qui disent: « Nos dossiers indiquent que vous pouvez voter par courriel, et voici comment vous pourriez le faire. » Je ne sais pas si cela a déjà été utilisé quelque part.

On y trouve des références au gouvernement canadien. Cela fait partie de la raison pour laquelle j'ai demandé plus tôt si vous aviez déjà songé à utiliser le téléphone, le courriel ou quoi que ce soit d'autre pour les élections. Il semble qu'on a fait un certain type de proposition à un certain moment donné, soit utiliser ce système de vote direct.

[*Français*]

M. Jacques Gourde: Plus on avance, plus on découvre des choses. Pensez-vous qu'il faudra adapter nos lois électorales en fonction de la nouvelle réalité d'aujourd'hui? Quels changements devrions-nous apporter à nos lois pour protéger les renseignements personnels et notre démocratie? Faudrait-il interdire carrément l'utilisation de ces nouveaux outils, puisque, compte tenu du contexte international, il serait trop facile de contourner les balises que nous pourrions fixer pour protéger notre démocratie contre l'utilisation de ces outils?

[*Traduction*]

M. Chris Vickery: Interdisons carrément le logiciel — c'est trop facile de contourner les balises et trop arbitraire d'essayer d'interdire le logiciel.

Je crois que, au final, la réponse sera la transparence. Ne pas permettre aux gens de se cacher dans l'ombre lorsqu'ils tentent d'influencer la population par des moyens qui pourraient être ou non douteux. Faire en sorte qu'il soit facile de découvrir qui se cache derrière une annonce ou une campagne particulière est d'une importance critique, et la traçabilité de l'argent qui a servi à payer cette campagne ou cette annonce est extrêmement importante.

Mis à part cela, je ne connais pas très bien les détails particuliers de la loi canadienne sur les élections, pour être franc, donc je ne sais pas quelles autres améliorations pourraient être apportées.

[*Français*]

M. Jacques Gourde: Ceux qui utilisent ces logiciels et toute l'information qui se trouve un peu partout sur Internet ont-ils vraiment un avantage marqué comparativement à ceux qui utilisent seulement les outils conventionnels et les informations fournies par les organismes de l'État, en l'occurrence Élections Canada?

[*Traduction*]

M. Chris Vickery: J'ai toujours cru que le fait d'exploiter la technologie vous donnait une longueur d'avance presque partout. C'est peut-être une de mes croyances philosophiques selon lesquelles les gens ont un avantage lorsqu'ils utilisent la technologie de développement de logiciels la plus récente et la meilleure. C'est juste un concept avec lequel je serais d'accord.

Il y a des niveaux en ce qui concerne l'exploitation. Vous pouvez utiliser un marteau pour construire une maison ou encore pour agresser quelqu'un. Cela ne veut pas dire que vous devriez éliminer complètement les marteaux.

[*Français*]

M. Jacques Gourde: Par contre, ceux qui utilisent ces logiciels ont accès à des informations plus poussées, et même à des informations qui concernent la vie privée des gens. Si certaines personnes ont accès à de telles informations, mais que d'autres, qui n'ont pas les moyens financiers d'utiliser ce genre de technologie, n'utilisent que celles fournies par Élections Canada, cela crée une certaine injustice. Il faut payer pour obtenir ces informations. Or, ce ne sont pas tous les partis ou tous les candidats qui peuvent se le permettre. Il y a des plafonds de dépenses électorales, mais dans plusieurs cas ils ne sont jamais atteints, simplement parce que les gens n'en ont pas les moyens. Il se crée donc une injustice. Ces personnes ne sont pas à armes égales au moment d'une élection ou au sein de notre démocratie. Plus ces logiciels plus ou moins permis feront des avancées, plus il y aura une démocratie à deux vitesses.

● (0935)

[*Traduction*]

M. Chris Vickery: Je dirais que c'est un concept qui peut être appliqué à beaucoup de choses différentes, et oui, c'est vrai que les gens qui ont plus d'argent ont tendance à être avantagés dans une élection. C'est un problème auquel les États-Unis font vraiment face. La Cour suprême des États-Unis a décidé que l'argent équivaut à la liberté d'expression, qui est une valeur sacro-sainte de nos principes de base.

C'est quelque chose à quoi on doit faire face. Je ne pense pas qu'il y ait une réponse facile quant à la façon de réglementer l'argent et l'avantage des gens qui ont de l'argent par rapport aux personnes qui n'ont pas d'argent dans une élection. Je ne crois pas qu'il y ait une réponse facile à cela.

[*Français*]

M. Jacques Gourde: Merci.

[*Traduction*]

Le président: Merci, monsieur Gourde.

La prochaine est Mme Vandenbeld.

Mme Anita Vandenbeld (Ottawa-Ouest—Nepean, Lib.): Merci beaucoup d'être ici de nouveau. Je pense que votre dernier témoignage a beaucoup guidé notre étude et que nous avons une meilleure idée de l'énormité de ce à quoi nous avons affaire ici.

Après avoir entendu votre témoignage, nous avons reçu M. Silvester. Je l'ai interrogé par rapport à ce que vous aviez dit sur le fait que la base de codes comportait certaines empreintes digitales. Je crois que vous avez dit qu'elle figurait parmi les clients. Il y avait des numéros d'identification qui montraient que SCL et AIQ utilisaient la même base de codes.

M. Silvester a répondu ceci: « Je ne sais pas à quoi faisait allusion le chercheur » — en se reportant à vous —, « mais je peux dire que les seuls renseignements que nous avons reçus de SCL pour la prestation de services pour SCL étaient destinés expressément aux campagnes pour lesquelles nous offrions notre aide ». Puis, il a ajouté: « nous ne conservons pas de renseignements personnels d'une campagne à l'autre », et enfin: « nous ne transmettons ces renseignements à personne, sauf aux gens qui nous les ont fournis ».

En ce qui a trait aux notes psychosociales de Ripon, il a dit qu'ils avaient une « note concernant la participation aux élections », mais ils ne l'ont pas transférée à qui que ce soit, et aussi que cela n'aurait pas pu se rendre à qui que ce soit d'autre par leur entremise. De plus, il a affirmé qu'ils ne conservaient aucune des données. Je le cite ici: « Nous ne sommes pas une entreprise de données, donc nous n'avons aucun intérêt à le faire. »

Que pensez-vous de la crédibilité de ses réponses?

M. Chris Vickery: Cela défie l'imagination de croire qu'une personne irait dire ces choses. Ils ont un grand intérêt dans les données. Dans le disque dur que je vous ai fourni, il y a des données qui prouvent qu'un grand nombre de ses affirmations sont inexactes. Je suis vraiment surpris de constater qu'il irait dire ces choses. J'imagine qu'il a pensé que je n'allais pas fournir au comité canadien des copies de ce qui s'y trouvait ou il doit du moins avoir espéré que je ne le ferais pas, parce que c'est simplement faux.

Mme Anita Vandenbeld: Merci de l'avoir fait.

Si vous pouviez précisément envoyer au Comité — parce que nous allons les inviter à nouveau — les choses qui permettraient de réfuter ce qu'il a dit, ce serait très utile.

Merci.

M. Chris Vickery: M. Baylis en a une copie, mais je vais l'envoyer à tout le Comité.

Mme Anita Vandenbeld: Merci.

Je vais partager mon temps avec M. Picard.

M. Michel Picard (Montarville, Lib.): Merci.

Rebonjour, monsieur Vickery. Comment allez-vous?

M. Chris Vickery: Je vais bien.

M. Michel Picard: J'ai deux brèves questions, mais elles sont un peu compliquées.

Je vais commencer par une comparaison. Lorsque nous examinons les systèmes de blanchiment d'argent, nous voyons que, dans certains cas, vous avez une foule d'entreprises dont la structure n'explique pas les activités commerciales. Ce n'est pas illégal de constituer en société des entreprises, mais le fait de trouver 10, 15 ou 20 entreprises dans une structure qui n'a pas besoin d'autant d'entreprises est un indice de quelque chose. Ce n'est pas une preuve, c'est un indice.

Si nous regardons ce que nous avons dans les données que vous avez examinées, ce n'est pas illégal d'avoir un code. C'est normal pour une société de commercialisation de développer un code afin de mieux connaître sa clientèle. Quels sont les indicateurs qui donnent à penser que, oui, c'est logique dans certains cas, mais dans notre cas, ça ne l'est pas, parce qu'il y a les indicateurs qui donnent à penser que, disons, quelque chose est louche?

Je pose la question, parce que l'ancien dirigeant du FBI, M. Comey, a dit cette semaine que le Canada sera probablement la prochaine cible des pirates russes. Ce n'est pas une opération que vous commencez un jour, au moment où vous vous réveillez en vous disant que c'est une bonne idée. Vous devez mettre en place un certain nombre de choses, un certain nombre d'indicateurs que nous devons examiner. Quels seraient ces indicateurs?

● (0940)

M. Chris Vickery: Je tiens à préciser que je ne suis pas un expert en espionnage international, loin de là. En ce qui concerne les indicateurs qui montreraient une activité comme celle que M. Comey a décrite, vous feriez probablement mieux de vous adresser à un expert dans ce domaine.

Je peux parler très clairement et de façon très approfondie des données qui sont présentes dans le GitLab d'AIQ, assurément, mais je ne voudrais pas avoir l'air d'un charlatan et essayer de deviner des signaux ou des indicateurs d'espionnage international. Je ne me crois pas qualifié en ce moment pour répondre à cette question.

M. Michel Picard: Permettez-moi d'atténuer un peu la pression sur vos épaules. L'idée n'est pas de voir s'ils nous épient ou non. Si je reviens à mon exemple de blanchiment d'argent, du point de vue des entreprises, du point de vue financier, tout le monde qui connaît son domaine de travail, les experts financiers diront que la constitution en société est une bonne chose et que les entreprises doivent se constituer en société pour certaines activités. Dans ce cas, je trouve étrange que cette personne ou ce groupe de personnes ait constitué en société 15 entreprises. Pour cette entreprise, c'est compliqué pour rien.

Si vous regardez ce que vous trouvez dans vos données, il est probable que les sociétés de commercialisation utilisent ces codes pour leurs fins. Qu'est-ce qui donne à penser que c'est correct dans un domaine de travail, mais pas dans un autre? Un des préjugés que nous avons lorsque nous essayons d'enquêter sur quelque chose, c'est que nous proposons une intention lorsqu'il n'y en a pas, mais nous ne voyons pas l'intention lorsqu'il pourrait y en avoir une.

En faisant une analyse pratique des données, nous pouvons dire que ces données sont logiques, mais dans ce cas-ci, nous ne comprenons pas pourquoi ces personnes utilisent ces types de données, parce que le contexte ne respecte pas le but de l'entreprise.

M. Chris Vickery: D'accord. Je crois que je comprends là où vous voulez en venir.

Une des choses originales qui ont attiré mon attention lorsque j'ai visité le site Web aggregateiq.com pour la première fois — je ne savais pas de qui il agissait — c'est qu'ils semblaient être dans le même secteur, la même industrie ou le même domaine que Cambridge Analytica. J'ai vu sur GitHub — c'est différent de GitLab — un code qui renvoyait à aggregateiq.com, où il était noté que Cambridge Analytica était client de SCL. On avait tendance à penser: pourquoi toutes les entreprises dans le même domaine coopèrent-elles? Elles ne se marchent pas sur les pieds? Cela n'avait pas beaucoup de sens pour moi. C'est une des choses qui ont au départ attiré mon attention.

Un autre élément important des fichiers de GitHub ou de GitLab, c'est qu'une politicienne américaine, dont le nom de famille est « McSally », semble avoir été cliente d'AIQ — ou c'est AIQ qui a travaillé sur sa campagne — tout en étant, je crois, cliente de Deep Root Analytics, qui est une autre entreprise d'analyse de données pour laquelle j'ai découvert une atteinte à la protection des données. S'il y a là un lien, est-il probable que les deux entreprises se coordonnaient d'une certaine façon pour l'aider dans sa campagne? Il me semble étrange qu'une campagne utiliserait deux entreprises semblables et que les entreprises ne se parleraient pas pour travailler à l'atteinte d'un but commun, donc cela contribue à renforcer l'idée de l'existence d'une plus grande machine au travail.

M. Michel Picard: Merci.

Le président: Le dernier à passer est M. Boulerice, pour trois minutes.

[*Français*]

M. Alexandre Boulerice: Je vous remercie encore une fois, monsieur Vickery.

Vous avez eu au cours des dernières semaines, par l'entremise de Twitter, certaines interactions intéressantes avec les gens de Facebook. Vous avez soulevé le fait que, malgré les déclarations rassurantes de Facebook, 14 applications d'AIQ étaient encore actives, alors qu'elles avaient été officiellement suspendues par Facebook. Les gens de Facebook vous ont répondu sur Twitter, vous remerciant et affirmant avoir finalement suspendu les 14 applications. Ils ont même osé vous dire de ne pas hésiter à utiliser leur programme de primes pour le signalement d'utilisations abusives de données, ce que je trouve assez ironique. Je ne sais pas si vous avez eu recours à ce système de primes.

Aujourd'hui, êtes-vous moins inquiet quant à la façon inappropriée dont certaines applications utilisent Facebook?

● (0945)

[*Traduction*]

M. Chris Vickery: Je suis heureux d'apprendre que Facebook semble être [*Difficultés techniques*] dans une bonne direction. Je ne suis pas du tout convaincu que l'infection ait été totalement éliminée. Il est probable qu'on trouve davantage d'applications qui procèdent à un certain type de blanchiment de la réputation, c'est-à-dire que c'est la même application malicieuse sous un nom différent et une apparence modifiée. Je pense que c'est très probable, et il faudra que Facebook déploie passablement d'efforts pour complètement débusquer tous les mauvais acteurs qui cherchent à profiter de la plateforme.

[*Français*]

M. Alexandre Boulerice: Étant des personnalités publiques, nous faisons tous, à des degrés divers, de la communication politique. Pour ce faire, nous utilisons les médias sociaux. Nous sommes, pour la plupart, inscrits à nombre de ces médias. Par ailleurs, certains d'entre nous sont parents. Pour ma part, j'ai des adolescents à la maison qui sont, eux aussi, présents sur certaines plateformes.

En matière de protection de la vie privée des gens et des renseignements personnels, j'aimerais savoir lequel de ces outils, selon vous, que ce soit Facebook, Twitter, Snapchat, Instagram ou d'autres, est le plus sécuritaire ou risque le moins d'être utilisé pour amasser des données qui serviront à des fins politiques par la suite.

[*Traduction*]

M. Chris Vickery: Toute entreprise qui est mue par le profit, ce qui n'est pas en soi une mauvaise chose, aura un incitatif pour maximiser ce profit pour ses actionnaires. Certains diraient même qu'elle a le devoir de le faire. La publicité, le profilage précis et la vente de données sont des façons de maximiser ces profits. Je ne crois pas qu'aucune de celles que vous avez mentionnées n'est nécessairement meilleure que l'autre ou plus axée sur la protection des renseignements personnels.

Je crois que nous devons modifier le comportement de l'industrie et changer en quelque sorte les priorités ou les incitatifs auxquels elle accorde la priorité; plutôt que d'être simplement obnubilée par le profit à tout prix, elle devrait se dire: « Si je suis moins stricte quant à la protection des renseignements personnels, je pourrais finir par me voir imposer des amendes par les organismes de réglementation, et mes profits ne seraient pas aussi élevés. Je ferais mieux de protéger les renseignements personnels des gens. »

C'est juste que la dynamique différente de la carotte et du bâton est, tout à fait, déréglée en ce moment.

Le président: Le temps est écoulé.

M. Nathaniel Erskine-Smith: Monsieur le président, nous avions au départ prévu passer à huis clos afin de discuter des travaux du Comité. Ma principale préoccupation, c'est que Peter et Charlie ne sont pas ici. Nous devons nous pencher sur des recommandations concernant les travaux du Comité, et je ne suis pas à l'aise, puisqu'ils ont travaillé de façon passablement non partisane, qu'ils ne soient pas ici pour faire ce travail.

Nous avons un peu de temps en ce moment. Peut-être que M. Vickery a un peu plus de temps. Il a dit qu'il a discuté à huis clos avec le comité du Royaume-Uni, et cela a été utile, dans une certaine mesure. Je me demande si nous pourrions prendre au moins une demi-heure et voir où cela nous mène. Si M. Vickery est en mesure de passer à huis clos, nous pourrions consacrer un certain temps à cela. Nous pourrions également tenir une autre discussion par la suite, si nous pouvons discuter autrement des travaux du Comité.

Le président: Oui. J'allais justement proposer de passer à huis clos avec M. Vickery pendant une certaine période. Nous verrons où cela nous mène, j'imagine, et utiliserons le temps que le Comité souhaite utiliser à huis clos.

M. Nathaniel Erskine-Smith: Excellent.

Le président: En ce qui concerne les recommandations, elles ont été fournies par tous les partis. Nous n'en avons pas nécessairement besoin ici, en personne, pour les passer en revue, mais s'il y a des désaccords au sujet de ces recommandations...

● (0950)

M. Nathaniel Erskine-Smith: Si on présume qu'il n'y a pas de conflits... oui, exactement.

Le président: ... donc nous devrons composer avec cela, j'imagine.

M. Nathaniel Erskine-Smith: C'est bon.

Le président: Si je comprends bien, toutefois, c'est assez simple.

Monsieur Vickery, avez-vous du temps pour passer à huis clos avec nous pendant quelques minutes?

M. Chris Vickery: Oui.

Le président: J'ai une question pour vous dans l'intérêt du public. Avez-vous regardé ce qui se passe au comité du Royaume-Uni, y compris hier, avec M. Collins et le témoin, M. Nix? Avez-vous eu la chance de voir le témoignage?

M. Chris Vickery: J'ai visionné le témoignage de M. Nix hier. J'ai dû prendre quelques pauses pour travailler un peu et assister à quelques conférences et d'autres choses, mais j'ai visionné une bonne partie de son témoignage.

Quant à la première personne que vous avez mentionnée, je crois que j'ai lu une partie de la couverture, mais je n'ai pas de connaissance particulière.

Le président: M. Nix est l'ancien responsable de Cambridge Analytica. Pour moi, c'était juste très intéressant. Cela m'a, en quelque sorte, frappé hier soir, lorsque je le regardais... Lorsque nous siégeons à la Chambre jusqu'à minuit, une chose que nous faisons, c'est regarder ce que le Royaume-Uni fait; je vais l'admettre. Mon inquiétude en tant que président — je pense que c'est ce que nous avons en commun en tant que présidents du côté des États-Unis et du Royaume-Uni — c'est que nous ne regardons que quelques entreprises. J'imagine que c'est mon inquiétude. Faisons-nous seulement un examen superficiel ici?

M. Chris Vickery: Oui. Nous, vous, chacun des comités, faisons un examen superficiel. Je crois fermement que nous découvrirons beaucoup plus de choses.

Le président: D'accord. Merci, monsieur Vickery.

Nous allons suspendre la séance, puis nous reprendrons à huis clos dans cinq minutes.

M. Chris Vickery: Cela me va.

Le président: Merci.

[*La séance se poursuit à huis clos.*]

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes
à l'adresse suivante : http://www.noscommunes.ca

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the
following address: http://www.ourcommons.ca